

13 July 1978

STATINTL MEMORANDUM FOR: [REDACTED] Assistant for Information, DDA  
[REDACTED] of Security, DDA  
[REDACTED] Director of Central Reference,  
[REDACTED], Policy & Coordination Staff,  
[REDACTED] al Assistant, DDS&T  
[REDACTED] Security Committee

STATINTL FROM : [REDACTED]  
Office of General Counsel

SUBJECT : Executive Order 12065: Implementing Directive

1. Attached is a 12 July 1978 draft of a directive to implement Executive Order 12065. This draft is the product of an informal working group coordinated by NSC to provide a framework from which to begin a more formal review of the requirements of the Order. Attached also are additional recommendations prepared by DoD that were considered at a recent meeting and incorporated in part into the draft.

2. I would appreciate your review of the attached, keeping in mind that we may recommend additional language, as well as comment on the draft as now written. It will be obvious to you that the draft is lacking in many respects. For example, there are some provisions in the Executive order which are not, but should be, addressed in this directive. If you have any specific recommendations, please prepare some language suitable for inclusion into the next version of the draft and the justifications therefor.

3. I have scheduled a meeting for Friday, 28 July 1978, in the DDS&T Conference Room, 6 E 60, from 2 to 5 P.M. At that meeting I expect we shall consider any specific recommendations and attempt to reach an informal consensus at the working level so that this Office may recommend further amendments prior to the directive's formal coordination by NSC. Since this will be essentially a mark-up session, only specific recommendations need be in writing.

4. For your information, I intend to be out of the office until the 28th. If you have any questions or comments prior to that time, please call [REDACTED] of this Office at extension [REDACTED]. Let me remind you also that the Agency is expected to have at least one more opportunity to make further changes or recommendations before the NSC circulates the directive around the Government for official review. Thank you very much for your cooperation.

STATINTL

STATINTL

STATINTL

STATINTL

Attachments

cc: [REDACTED]

NATIONAL SECURITY COUNCIL  
DIRECTIVE  
CONCERNING  
NATIONAL SECURITY INFORMATION

July 12, 1978

The President has directed that Executive Order 12065, "National Security Information," dated June 28, 1978, be implemented in accordance with the following:

I. ORIGINAL CLASSIFICATION

- A. Definition. "Original classification" as used in the order means an initial determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure coupled with a designation signifying that such a determination has been made.
- B. Authority to Classify. In the absence of an authorized classifier the person designated to act in his/her absence may exercise the classifier's authority.
- C. Request for Classification Authority. Requests for original classification authority to Agencies not listed in Section 1-2 of the Order shall be submitted to the President through the Information Security Oversight Office. Requests shall include: (1) the designation of the official or position for which authority is sought; (2) the level of authority requested; and (3) justification for the granting of authority to include

the type of information originated by the Agency which requires original classification and an estimate of the number of original classification actions which the Agency will initiate annually.

D. Record Requirements. Agencies granted original classification authority pursuant to Section 1-2 of the Order shall maintain a current listing, by classification designation, of officials or positions designated in writing as original classifiers. If the listing of the names of officials having classification authority discloses intelligence information, the agency may, with the approval of the Director of the Information Security Oversight Office, establish some other means by which such officials can be readily identified.

E. Classification Procedure. Original classification is a two-step procedure. Every original classification must include, first, a determination that the information concerns one or more of the categories of subject matter described in or designated pursuant to Section 1-301 of the Order; and second, a determination that disclosure of the information reasonably could be expected to result in one of the three categories of damage described in Section 1-1 of the Order. The determination involved in the first step is separate and distinct from that of the second. The fact that the information falls under one or more of the qualifying categories shall not be presumed to mean that the information automatically meets the damage criteria.

F. Standard Identification and Markings. Information originally classified pursuant to the Order shall, at the time of origin, be marked as follows:

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

(1) Date of Classification and Office of Origin. A date and office of origin on a document at the time of its origination in compliance with agency standards and procedures prescribed for preparation of such documents is deemed to be the date of classification and identification of the office of origin of classification of any originally classified document.

(2) Identity of Classifier. The identity of the classifier, unless also the signer or approver of the document, shall be shown on a "classified by" line, e.g., "classified by (John Doe)" or classified by "Director, XXX."

(3) Date or event for Declassification or Review. The date for automatic declassification or for declassification review shall be shown on a "declassification on" or a "review for declassification on" line, e.g., "declassify on 1 November 1984," "declassify on Completion of State Visit," or "review for declassification on 1 November 1998."

(4) Identity of Extension Authority. The identity of the official who authorized a date for declassification or for review for declassification that is more than six years beyond the date of the document's classification shall be shown on the document unless the extension authority also is the classifier, signer or approver of the document. This marking shall be shown substantially as follows: "Extended by (insert name or title of position of agency head or TS authority)."

(5) Reason for Extension. Agency regulations shall establish criteria for determining whether classification may be extended beyond six years. The reason for extension may be shown on documents by citing the part of the agency regulation which states the applicable criterion, substantially as follows: "Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5" (insert applicable reference to agency regulation)."

(6) Mandatory Portion Marking. Classifiers shall, through marking or other means, identify (a) the level of classification of each classified portion of a document, and (b) those portions which are not classified. Portion marking shall be parenthetical and shall be placed so as to immediately precede or follow the text of each respective portion. The symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used for this purpose. When individual portion marking is clearly impracticable, classifiers may, through the use of a conspicuous notation on the document specify the classification level of the various information elements in the document. Each portion need not be separately marked if all portions of a classified document are classified at the same level and a statement to that effect is included in the document. A specific waiver of the portion marking requirement may be granted by the Director of the Information Security Oversight Office. Requests for such waivers shall be made by the head of an agency to the Director together with (a) specific identification of the information for which such waiver is sought, and (b) detailed explanation of why the agency should not comply with the marking requirement, and (c) the agency's best judgment as to the anticipated dissemination of the information, and the extent that the information may form a basis for classification of other documents.

(7) Overall and Page Marking of Documents. The overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked, stamped, or permanently affixed at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the

outside of the back cover (if any). Each interior page of a classified document shall be conspicuously marked or stamped at the top and bottom either (a) according to the highest classification of the content of the page, including the designation "Unclassified" when appropriate or (b) in special situations (e.g. the marking of voluminous printed documents) the highest overall classification of the document. In the latter case, portion marking of each page shall take precedence over page marking.

(8) Subjects and Titles. Whenever possible, subjects and titles shall be selected so as not to require classification. Classification status of subjects and titles of classified documents shall be identified by use of the parenthetical symbols shown in (6) above. When the subject or title is classified, an unclassified identifier may be assigned to facilitate receipting and reference purposes.

(9) Material Other Than Documents. The classification and associated markings prescribed by this Directive for material other than documents shall, where possible, be conspicuously affixed to the material by stamping, tagging or other means. When such is not possible, recipients shall be made aware of the classification and associated markings by notification or other means as prescribed by Agency regulations.

(10) Transmittal Documents. A transmittal document shall indicate on its face the highest classification of the information transmitted by it, and the classification, if any, of the transmittal document, standing alone. For example, an unclassified transmittal document should bear a notation substantially as follows: "UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS DETACHED."

(11) Downgrading Markings. Whenever it is determined that automatic downgrading of an assigned classification designation will serve a useful

purpose, the date for taking such action shall be shown on the face of the document containing the information, e.g., "Downgrade to Secret on 1 November 1990" or "Downgrade to Confidential on 1 December 1985".

G. Additional Markings Required. In addition to the foregoing marking requirements, the following markings shall be prominently displayed on classified information, as appropriate to its contents as prescribed below. When display of these additional markings is not feasible, their applicability to the information shall be included in the written notification of the assigned classification.

(1) Restricted Data. For classified information containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended:

"RESTRICTED DATA"

"This document contains Restricted Data  
as defined in the Atomic Energy Act of  
1954. Its dissemination or disclosure  
to any unauthorized person is prohibited."

(2) Formerly Restricted Data. For classified information containing Formerly Restricted Data, as defined in Section 142 d., Atomic Energy Act of 1954, as amended, but containing no Restricted Data:

"FORMERLY RESTRICTED DATA"

"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination.  
Section 144b., Atomic Energy Act, 1954."

(3) Intelligence Sources and Methods Information. For classified information on sensitive intelligence sources or methods:



(4) Dissemination and Reproduction Notice. For classified information which the originator has, pursuant to Section 1-506 of the Order, determined should be subject to special dissemination and reproduction limitations, a statement substantially as follows shall be included in the document or on its cover sheet:

"Reproduction controlled by originator or higher authority.

Dissemination controlled by addressee."

Reproduction of all or portions of the information contained in documents so marked is prohibited without authorization of the originating office or higher authority. Further dissemination within the receiving agency is restricted to persons authorized by the addressee. Other notations of restrictions on reproduction, dissemination or extraction of classified information, e.g., markings to indicate information falls within a special access program, may be prescribed by Agency regulations.

## II. DERIVATIVE APPLICATIONS OF CLASSIFICATION MARKINGS

A. Definition. "Derivative classification" as used in the Order means a determination by any individual responsible to do so that official information is in substance the same as information known by that person to be already classified or identified by the government as Top Secret, Secret or Confidential and designates it accordingly.

B. Responsibility. Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information which is already classified or those who apply markings in accordance with guidance from an authorized classifier. Persons who apply derivative classifications should take care to determine whether their paraphrasing, restating or summarizing of classified information has removed all or part of the basis for classification. Where checks with originators or other appropriate inquiries show that no classification or a lower classification than originally assigned is appropriate, the information shall be marked accordingly.

C. Marking Derivatively Classified Documents. At the time they are originated, paper copies of derivatively classified documents shall be marked as follows:

- 1 The classification authority shall be shown on a "Classified by" line, e.g., "Classified by (Identity of Classification Guide)" or

"Classified by (Source of original classification)." In the latter example, if the classification is derived from more than one source, the single phrase, "multiple sources," may be shown provided that identification of all such sources is maintained with the file or record copies of the document.

(2) The identity of the office originating the derivatively classified document will be shown on the face of the document.

(3) Dates or events for declassification or review will be carried forward from the source material or classification guide and shown on a "Declassify on" or "Review for Declassification on" line. In the case of information classified on the basis of multiple sources, the most restrictive of the declassification dates applicable to the various source material used shall be applied to the new information.

(4) Any special notation appearing on the source material, e.g., special access restrictions, Restricted Data or Formerly Restricted Data, shall be carried forward to the new material when appropriate.

(5) Overall, page and portion classification marking requirements prescribed for originally classified documents in Section I. F. (6) and (7) are also applicable to derivatively classified documents.

### III. CLASSIFICATION GUIDES

A. Guidance Requirements. Classification guides promulgated shall:

(1) Identify the information elements to be protected, using categorization and sub-categorization to the extent that the

information involved can be readily and uniformly identified;

(2) State which of the classification designations (i. e., Top Secret, Secret, or Confidential) apply to the identified information element;

(3) State the duration of each such specified classification in terms of a period of time or future event. When such duration is to exceed six years, the specific reason for such extension shall, unless classified, be provided in the guidance in accordance with the provisions of Section 1-502 of the Order. Classified reasons shall be included on the record copy of the guidance.

B. Review and Report Requirements. All classification guides shall be reviewed for currency and renewed or revised on an annual basis. A master list of all classification guides issued by each Agency listed in Section 1-2 of the Order shall be maintained at a central point in that Agency.

A. Record Requirements. Rosters shall be maintained of officials designated as declassification authorities pursuant to Section 3-103 of the Order. These rosters shall be subject to review by the Information Security Oversight Office.

B. Earliest Possible Declassification. Original classifiers may specify declassification dates or events at the limit of their authority (specified in Section 1-4 of the Order) only where a specific determination has been made that earlier declassification should not be accomplished.

C. Systematic Review for Declassification

(1) Systematic Review Guidelines

a. U. S. Originated Information. Heads of Agencies listed in Section 1-2 of the Order, heads of Agencies which had classification authority under previous Executive Orders, and officials designated by the President pursuant to Section 1-2 of the Order shall ensure that systematic review guidelines for 20-year-old information are prepared and promulgated after consultation with the Archivist of the United States and otherwise in accordance with Section 3-402 and 5-402 of the Order. Systematic Review Declassification guidelines shall be kept current. They shall be reviewed at least every other year and revised as necessary unless earlier review for revision is requested by the Archivist of the United States. Each Agency shall furnish a copy of its declassification guidelines and revisions thereto to the Information Security Oversight Office for review.

b. Foreign Government Information. In consultation with the Archivist of the United States and, when appropriate, with foreign governments or international organizations, heads of agencies shall develop and promulgate systematic review guidelines covering foreign government information. These guidelines shall be promulgated not later than one year after the effective date of the Order and shall be kept current through review by concerned agency heads every other year unless earlier review for revision is requested by the Archivist of the United States. A copy of the foreign government information guidelines and any revisions thereto shall be furnished to the Information Security Oversight Office. The Department of State will provide advice and such

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
assistance as is necessary to effect foreign government coordination of  
the guidelines.

(2) Systematic Review Procedures

a. Action on 20-year-old material. To conserve Government resources devoted to the systematic review of 20-year-old information and to achieve more effective declassification, only material constituting the permanently valuable records of the Government, in accordance with 44 U.S.C. 2103, shall be subjected to systematic review for declassification. Within 60 days of the effective date of the Order heads of agencies and officials designated by the President pursuant to Section 1-2 of the Order shall direct that all security classified records 20 years old or older, whether held in storage areas by the agency or in Federal records centers be surveyed to identify those that require scheduling for future disposition. Such scheduling must be accomplished within two years of the effective date of the Order.

b. Extending Classification After Review. Only the head of an agency that originated the information, or of an agency which is the successor to a defunct agency that originated the information, or of an agency of primary interest, or an official designated by the President pursuant to Section 1-2 of the Order, is authorized to extend the classification of U. S. originated information beyond 20 years. Only the Head of an Agency with primary interest is authorized to extend the classification of foreign government information beyond 30 years. This authority may not be delegated, but the senior agency official responsible for the Information Security program may be assigned responsibility for the performance of administrative functions necessary to effect the extension of classification beyond 20 years or beyond 30 years as the case may be.

c. Assistance to the Archivist. The head of each Agency shall designate experienced personnel to assist the Archivist of the United States in the systematic review of 20-year-old U. S. originated information and 30-year-old foreign information. Such personnel shall:

i. Provide guidance and assistance to National Archives employees in identifying and separating documents and specific categories of information within documents which are deemed to require continued classification; and

ii. Develop reports and lists for submission to the head of the Agency which identify the documents and categories of information so separated, with recommendations concerning continued classification.

The head of the Agency will then make the determinations required under Section 3-401 of the Order as to which documents and categories of information require continued protection personally and in writing to the Archivist of the United States. Included in the determinations will be a specification of the dates on which such documents and categories of information shall be automatically declassified or reviewed again.

(3) Waivers of Further Review

Heads of Agencies listed in Section 1-2 and officials designated by the President pursuant to Section 1-201 of the Order may request a waiver of the ten-year review requirement from the Director of the Oversight Office. Such requests shall include personal certification by the Agency head that the classified information for which the waiver is sought was systematically reviewed as required, that a definitive date for declassification could not then be determined, and that the results of the review established an identifiable need to retain continued classification for a period in excess of twenty



additional years and a recommendation on the period before the next required review.

(4) Foreign Relations Series

In order to permit the editors of Foreign Relations of the United States to meet their mandated goal of publishing twenty years after the event, heads of departments and agencies are requested to assist the editors in the Department of State by facilitating access to appropriate classified materials in their custody and by expediting declassification review of items from their files selected for publication.

D. Procedures for Mandatory Declassification Review

(1) Action on an Initial Request

Each agency shall designate in its implementing regulations, that are published in the Federal Register, an office to which requests for mandatory review for declassification may be directed.

a. General Provisions. In addition to the provisions of Section 3-5 of the Order, the following procedures apply to mandatory review requests:

i. The designated office shall promptly acknowledge to a requestor the receipt of the request.

ii. Whenever a request does not reasonably describe the information sought or involves a large number of individual documents originated by numerous classifying authorities and requiring extensive coordination for review, the requestor shall be asked to provide additional information or to narrow the scope of the request. If thereafter the requestor does not describe the information sought with sufficient particularity, or does not narrow the scope of the request, he shall be notified that no review will be undertaken.

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

b. Information in the custody of and under the exclusive declassification authority of an agency. The designated office shall determine whether, under the declassification provisions of Section 3-3 of the Order, the requested information may be declassified and shall promptly notify the requestor of the determination and make the information available. If the information remains classified in whole or in part, the requestor shall be given a brief statement as to the reasons for the continued classification and a notice that he has the right to appeal the determination to a designated agency appeal authority (including name, title, and address of such authority) and that such an appeal must be filed with the agency within 60 days in order to be considered.

c. Information Classified by Agencies Other Than The Custodial Agency. When the designated office receives a request for information in a document which is in the custody of its agency but which was classified by another agency, that office shall refer the request to the designated office of the classifying agency, together with a copy of the document containing the information requested and shall notify the requester of the referral. The designated office of the reviewing agency shall review the document in coordination with any other classifying agencies. Where appropriate that office shall then respond to the request in accordance with the pertinent procedures described above and, if requested, shall notify the designated office of the referring agency of its determination.

d. Action on Appeal. The head of an agency, or his designee, shall establish procedures to act within 30 days upon all appeals of denials of requests for declassification. In accordance with those procedures the agency shall determine whether continued classification is required in whole

or in part and shall notify the requester of the determination and make available any authorization determined to be releasable. If continued classification is required under the provisions of Section 3-3 of the Order, the requester shall be notified of the reason therefor. If requested the agency shall also promptly communicate the appeal determination to any referring agency.

E. General Procedures for Changing Classification

(1) E. Challenges to Classification. Agency programs established to implement the Order shall encourage holders of classified information to challenge the classification in cases where there is substantial reason to believe that the information is classified unnecessarily or that overly restrictive periods for continued classification have been assigned. These programs shall provide for action on such challenges or appeals relating thereto within thirty days of receipt and for notification to the challenger of the results. When requested, anonymity of the challenger shall be preserved.

(2) F. Changes in Level or Duration of Classification

DD  
write  
(1)(X) Upgrading of Classification. The upgrading of classified information to a higher level than previously determined is permitted if (i) all known holders of the information can be notified promptly and (ii) all known holders of the information are authorized access to the higher level of classification, or, the information can be retrieved from all known holders of the information not authorized access to the contemplated higher level of classification.

(b)(2) Extension of Duration of Classification. The duration of classification specified at the time of original classification may be

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

extended by officials with requisite authority but only if notification of such action can be received by all known holders of the information prior to the date or event previously set for declassification.

(3) Notification. Notification of unscheduled downgrading, upgrading or change in duration may be by general rather than personal notice so long as the general notice is designed to achieve the intended result.

(4) Posted Notice. If prompt remarking of large quantities of information would be unduly burdensome, the custodian may attach declassification, downgrading, or upgrading notices to the storage unit in lieu of the remarking action otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action and the storage units to which it applies. Items withdrawn from such storage units shall be promptly remarked in accordance with the marking provisions herein. However, when information subject to a posted downgrading, upgrading or declassification notice is withdrawn from one storage unit solely for transfer to another, or a storage unit containing such information is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

## V. SAFEGUARDING

A. General. Information classified pursuant to this or prior Orders shall be afforded a level of protection against unauthorized disclosure commensurate with the level of classification and with its movement or transmission, storage, dissemination, use, and destruction.

B. Access Limitations. Access to classified information shall be granted only in accordance with the following:

(1) Determination of Trustworthiness. A person is eligible for access to classified information only if the person's reliability and trustworthiness are such that permitting the person access to classified information is clearly consistent with the national interest. This determination shall be made based on appropriate investigation as determined by the heads of Agencies in accordance with the standards and criteria of applicable Executive orders.

(2) Determination of Need-to-Know. Subsequent to the determination of trustworthiness, classified information shall not be made available to a person unless the possessor of the classified information establishes in each instance except as provided in Section 4-3 of the Order that access is essential to the accomplishment of official Government duties or contractual obligations.

(3) Access by Historical Researchers and Former Presidential Appointees. If the access requested by historical researchers and former Presidential appointees requires the rendering of services for which fair and equitable fees may be charged pursuant to Title 5 of the Independent Offices Appropriations Act, 1952, 65 Stat. 290, 31 U.S.C. 483a, the requester shall be so notified and the fees may be imposed. Agencies shall obtain the requester's written agreement to safeguard the information to which he is given access as required by the Order and implementing Directives and written consent to review of his notes and manuscript for the purpose of determining that no classified information is contained therein.

C. Dissemination

(1) Consent of Originating Agency to Dissemination by Recipient. Except as otherwise provided by Section 102 of the National Security Act of 1947, 61 Stat 495, 50 U.S.C. 405, classified information or material originating in one agency shall not be disseminated outside any other agency to which it has been made available without the consent of the

originating agency. The Department of Defense shall be considered as one agency in applying the foregoing rule.

(2) Dissemination of Intelligence Information. Information or material bearing the marking "WARNING NOTICE - SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" shall not be disseminated in any manner outside authorized channels without the permission of the originating Agency and an assessment by the senior intelligence official in the disseminating Agency as to the potential risks to the national security and to the intelligence sources and methods involved.

D. Accountability Procedures

(1) Stringent controls shall be placed on information classified Top Secret.

a. Top Secret Control Officers. Top Secret Control Officers shall be designated, as required, to receive, maintain current accountability and access records of, and dispatch Top Secret material.

b. Physical Inventory. A physical inventory of all Top Secret material shall be made at least annually. However, heads of Agencies may authorize the annual inventory of Top Secret information in repositories, libraries or activities which store large volumes of such information to be limited to documents to which access has been afforded within the past twelve months.

Secret and Confidential

(2) Current Accountability. Classified information shall be subject to such controls and current accountability records as the head of the Agency may prescribe.

E. Storage. Classified information may be stored only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it.

(1) Storage of Top Secret. Top Secret information shall be stored in a safe-type steel file cabinet having a built-in three-position dial type combination lock or in a safe-type vault, or vault-type room secured by a comparable lock, or in other storage facility which meets the standards for Top Secret established under the provisions of (3) below. In addition, heads of Agencies shall prescribe such additional, supplementary controls as are deemed appropriate to restrict unauthorized access to areas where such information is stored.

(2) Storage of Secret or Confidential. Secret and Confidential information may be stored in a manner and under the conditions prescribed for Top Secret information, or in a container or vault which meets the standards for Secret or Confidential, as the case may be, established pursuant to the provisions of (3) or (4) below.

(3) Standards for Security Equipment. The General Services Administration shall, in coordination with Agencies originating classified information establish and publish uniform standards, specifications and supply schedules for containers, vaults, alarm systems and associated security devices suitable for the storage and protection of all categories of classified information. Any agency may establish for use within such agency more stringent standards. Whenever new security equipment is procured, it shall be in conformance with the foregoing standards and specifications



and shall, to the maximum extent practicable, be of the type designated on the Federal Supply Schedule, General Services Administration.

(4) Exception to Standards for Security Equipment. As an exception to (3) above, Secret and Confidential information may also be stored in a steel filing cabinet having a built-in, three-position, dial-type changeable combination lock, or a steel filing cabinet equipped with a steel lock bar, provided it is secured by a padlock approved by GSA for the purpose. The storage of Secret information in a steel filing cabinet equipped with a steel lock bar, requires the use of such supplementary controls as the head of the Agency deems necessary to achieve the degree of protection warranted by the sensitivity of the information involved.

(5) Combinations

a. Equipment in Service. Combinations to dial-type locks shall be changed only by persons having appropriate security clearance, and shall be changed whenever such equipment is placed in use, whenever a person knowing the combination no longer requires access to the combination, whenever a combination has been subjected to possible compromise, at least once every year and whenever the equipment is taken out of service. Knowledge of combinations protecting classified information shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information to be stored in the security equipment concerned.

b. Equipment Out of Service. When taken out of service, security equipment having built-in combination locks shall be reset to

the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30.

(6) Keys. Heads of Agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated high security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected. Under no circumstances shall keys be removed from the premises or stored except in a secure container.

(7) Responsibilities of Custodians. Persons entrusted with classified information shall be responsible for providing protection and accountability for such information at all times and particularly for locking classified information in approved security equipment whenever it is not in use or under direct supervision of authorized persons.

Custodians shall follow procedures which insure that unauthorized persons do not gain access to classified information by sight or sound.

(8) Inspections. Individuals charged with the custody of classified information shall conduct the necessary inspections within their areas to ensure adherence to all procedural safeguards prescribed to protect classified information. In addition, Agency security officers shall ensure that periodic inspections are scheduled to ensure that procedural safeguards prescribed by Agency regulations are taken to protect classified information at all times.

G. Transmission

(1) Preparation and Receipting. Classified information shall be enclosed in opaque inner and outer covers before transmitting. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document, but shall contain no classified information. It shall be signed by the recipient and returned to the sender.

(2) Transmission of Top Secret. The transmission of Top Secret information shall be effected preferably by oral discussion in person between the officials concerned, in an appropriately secure area. Otherwise the transmission of Top Secret information shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for that purpose, over authorized communications circuits in encrypted form or by other means authorized by the National Security Council.

(3) Transmission of Secret. The transmission of Secret material shall be effected in the following manner:

a. The Fifty States, District of Columbia, Puerto Rico.

Secret information may be transmitted within and between the fifty States, District of Columbia and Puerto Rico by one of the means authorized for

Top Secret information, by the United States Postal Service registered mail

and by protective services provided by the United States air or surface commercial carriers under such conditions as may be prescribed by the head of the Agency concerned.

b. Other Areas, Vessels, Military Postal Services, Aircraft.

Secret information and material may be transmitted from, to or within areas other than those specified in a, above, by one of the means established for Top Secret information and material or; by United States registered mail through Army, Navy or Air Force Postal Service facilities provided that the material does not at any time pass out of United States citizen control and does not pass through a foreign postal system. Transmission outside such areas may also be accomplished under escort of appropriately cleared personnel aboard United States Government and United States Government contract, vehicles, aircraft, ships of the United States Navy, civil service manned U. S. Naval ships and ships of U. S. Registry, Operators of vehicles, captains or masters of vessels and pilots of aircraft, who are United States citizens and who are appropriately cleared, may be designated as escorts.

c. Canadian Government Installations. Secret information may be transmitted to and between United States Government and Canadian Government installations in the fifty States, the District of Columbia and Canada by United States and Canadian registered mail with registered mail receipt.

(4) Transmittal of Confidential. Confidential information and material shall be transmitted within the forty-eight contiguous states and

the District of Columbia, or wholly within Alaska, Hawaii, the Commonwealth of Puerto Rico, or a United States possession, by one of the means established for higher classifications, or by certified or first class mail when prescribed by an agency head. Outside these areas, Confidential information and material shall be transmitted only as is authorized for higher classifications.

(5) Transmission within an Agency. Agency regulations governing the preparation and transmission of classified information within an Agency shall ensure a degree of security equivalent to that prescribed above for transmission outside the Agency.

(6) Telecommunications Conversations. Classified information shall not be communicated over telecommunications circuits or systems other than those specifically authorized for transmission of classified information pursuant to subsection G(2) above.

H. Loss or Possible Compromise. Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated by his Agency or organization. In turn, the originating Agency shall be notified about the loss or possible compromise in order that a damage assessment may be conducted and appropriate measures taken to negate or minimize the adverse effect of such a compromise. An immediate inquiry shall be initiated by the Agency under whose cognizance the loss or compromise occurred for the purpose of

taking corrective measures and appropriate administrative, disciplinary, or legal action.

I. Destruction. Non-record classified information or material which has served its intended purpose shall be destroyed in accordance with procedures and methods approved by the head of the Agency. The method of destruction selected must preclude recognition or reconstruction of the classified information or material.

#### VI. COMBAT OPERATIONS

The provisions of the Order and this Directive with regard to dissemination, transmission, or safeguarding of classified information or material may be so modified in connection with combat or combat-related operations as the Secretary of Defense may by regulations prescribe.

#### VII. PUBLICATION AND EFFECTIVE DATE

This Directive shall be published in the Federal Register and become effective December 1, 1978.

The following organizational and other changes to the July 12, 1978 draft of the NSC Directive are submitted:  
Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

- o Add a Table of Contents, which could be more detailed than below, at the beginning of the Directive to read substantially as follows:

#### TABLE OF CONTENTS

#### I. ORIGINAL CLASSIFICATION

- A. Definitions.
- B. Authority to Classify.
- C. Request for Classification Authority.
- D. Record Requirements.
- E. Classification Procedure.
- F. Standard Identification and Markings.
- G. Additional Markings Required.
- H. Exception for Electrically Transmitted Messages.

#### II. DERIVATIVE APPLICATIONS OF CLASSIFICATION MARKINGS

- A. Definition.
- B. Responsibility.
- C. Marking Derivatively Classified Documents

#### III. CLASSIFICATION GUIDES

- A. Guidance Requirements.
- B. Review and Report Requirements.

#### IV. OTHER CLASSIFICATION ACTIONS AND NOTICES

- A. Challenges to Classification.
- B. Upgrading of Classification.
- C. Classification of Information Previously Determined to be Unclassified.
- D. Extension of Duration of Classification.
- E. Notification.
- F. Posted Notice.

#### V. DECLASSIFICATION

- A. Record Requirements.
- B. Earliest Possible Declassification.
- C. Systematic Review for Declassification.
- D. Procedures for Mandatory Declassification Review.

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
VI. SAFEGUARDING

- A. General.
- B. Access Limitations.
- C. Dissemination.
- D. Accountability Procedures.
- E. Storage.
- F. Transmission.
- G. Loss or Possible Compromise.
- H. Destruction.

VII. TREATMENT OF FOREIGN GOVERNMENT INFORMATION

- A. Identifying "Foreign Government, Information."
- B. Classification.
- C. Declassification.
- D. Safeguards.

VIII. COMBAT OPERATIONS

IX. PUBLICATION AND EFFECTIVE DATE

- o Add a new Section I.H. as follows:

H. Exception for Electrically Transmitted Messages. All classified messages transmitted via encrypted electrical means shall show: (1) the overall classification of the message; (2) parenthetical or other means of identifying the classification of its portions; and (3) either a date for declassification or a date for review for declassification. All other marking requirements of Sections 1-501 and 1-502 of the Order shall be deemed to be satisfied for messages if the copy prepared for transmission is completely marked as required for ordinary documents.

- o Add a new major Section IV entitled "Other Classification Actions and Notices" to be comprised of the present Section IV.E. plus new coverage with respect to classifying information previously determined to be unclassified. Insertion of this new major Section IV will require redesignation of the present Section IV as Section V, etc., as shown in the proposed Table of Contents.



- 3-607
- A. Challenges to Classification. Agency programs established to implement the Order shall encourage holders of classified information to challenge the classification in cases where there is substantial reason to believe that the information is classified unnecessarily or that overly restrictive periods for continued classification have been assigned. These programs shall provide for action on such challenges or appeals relating thereto within thirty days of receipt and for notification to the challenger of the results. When requested, anonymity of the challenger shall be preserved.
- B. Upgrading of Classification. The upgrading of classified information to a higher level than previously determined, by officials with requisite authority, is permitted if (i) all known holders of the information can be notified promptly and (ii) all known holders of the information are authorized access to the higher level of classification, or the information can be retrieved from all known holders not authorized access to the contemplated higher level of classification.
- 1-606
- C. Classification of Information Previously Determined to be Unclassified. Unclassified information, once communicated as such, is permitted to be classified only when the classifying authority makes the same determinations described for upgrading in Section IV.A. above and in addition, determines that control of the information has not been lost by such communication and can still be prevented from being lost.
- 1-401
- D. Extension of Duration of Classification. The duration of classification specified at the time of original classification may be extended by officials with requisite authority but only if notification of such action can be

received by all known holders of the information prior to the date or  
Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
event previously set for automatic declassification.

3-101 E. Notification. Notification of unscheduled downgrading, upgrading or change of duration of classification may be by general rather than personal notice so long as the general notice is designed to achieve the intended result.

3-101 F. Posted Notice. If prompt remarking of large quantities of information would be unduly burdensome, the custodian may attach declassification, downgrading, or upgrading notices to the storage unit in lieu of the remarking action otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action and the storage units to which it applies. Items withdrawn from such storage units shall be promptly remarked in accordance with the marking provisions herein. However, when information subject to a posted downgrading, upgrading or declassification notice is withdrawn from one storage unit solely for transfer to another, or a storage unit containing such information is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

- o The present Section IV.C.(1)b. (at the bottom of page 11a) is eliminated as its essence has been incorporated into the new major Section VII entitled "Treatment of Foreign Government Information." As a companion to this deletion, the text of the present Section IV.C.(1)a. must be inserted after the title (Systematic Review Guidelines) of the present Section IV.C.(1). The existing "a. U.S. Originated Information." is eliminated.

- o Add a new major Section VII (which consolidates and expands upon provisions of the draft applicable to foreign government information only). Insertion of this new major Section VII will require redesignation of the present Section VII as Section VIII, etc., as shown in the proposed Table of Contents.

VII Treatment of Foreign Government Information

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

1-301  
A. Identifying "Foreign Government Information." To be "foreign government information" within the meaning of the Order, information must be determined to be in one of two categories:

(1) Information provided to the United States by a foreign government or international organization <sup>of governments</sup> if as a condition precedent to acquisition <sup>, express or implied,</sup> ~~of it~~ the United States undertook an obligation to keep the information in confidence. Such an undertaking need not be written and the information <sup>provided</sup> is delivered in confidence if it is marked in a manner indicating it is to be treated in confidence or if the <sup>circumstances</sup> ~~terms~~ of the delivery <sup>indicate</sup> ~~specify~~ that the information <sup>is to</sup> be kept in confidence.

(2) Information <sup>produced</sup> by the United States pursuant to a written joint arrangement with a foreign government or international organization <sup>of go</sup> that requires confidentiality. A written joint arrangement <sup>may</sup> ~~must~~ be <sup>evidenced</sup> ~~executed~~ by ~~one of the parties to the arrangement and may be~~ an exchange of letters, a memorandum of understanding, or other informal written record of the joint arrangement.

B. Classification.

1-302(6)  
(1) Classification Procedure. The two-step procedure for classification prescribed in Section I.E. does not apply to the classification of foreign government information. With respect to such information, a presumption of at least identifiable damage is contained in Section 1-303 of the Order. ~~This must not be construed to mean that all foreign government information should be classified at the CONFIDENTIAL level.~~ Rather, at the time of classification, a determination <sup>may</sup> ~~should~~ be made <sup>that</sup> ~~as to whether~~ a higher classification would be appropriate. This determination will be

matter and the impact of its unauthorized disclosure to both the United States and the country or organization of origin.

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

(2) Duration of Classification. Unless the guidelines developed pursuant to Section 3-404 of the Order prescribe dates or events for declassification or for review for declassification:

a. Foreign government information will not be assigned a date or event for automatic declassification unless such is specified or agreed to by the foreign government.

b. All such information will be assigned a date for review for declassification at thirty years from the time the information was originated by the foreign government or acquired or classified by the United States, whichever is earlier.

NO  
No agreement.  
1-505

(3) Marking. Foreign government information incorporated in United States documents <sup>may</sup> ~~will~~, whenever practicable, be portion marked to reflect the country or international organization of governments of origin and the appropriate classification, e.g., "NATO(S)" or "U.K.(C)." <sup>in lieu of part</sup> ~~When such~~ <sup>marking</sup> marking is not practicable, the origin of foreign government information <sup>may</sup> ~~shall~~ be clearly indicated on or in the body of the material to assure that the information is not prematurely declassified nor made accessible to nationals of a third country without consent of the originator.] Foreign government documents classified by the foreign government will, if the foreign classification is not in English, be marked with the equivalent English classification. Foreign government documents not classified by the foreign government but provided to the United States in confidence

will be classified at an appropriate level and marked with the United  
States Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

OUT (4) Classification Guides. Original classification authority may be exercised with respect to foreign government information through classification guides. Such guides may describe categories of information or documents that are to be treated as foreign government information and may prescribe the classification that meets the requirements of Section 1-505 of the Order and Section VII.B. hereof. ]

C. Declassification.

Amend  
to 3-303  
✓  
(1) Balancing Test. In weighing the need to protect foreign government information ~~against the possible public interest in disclosure as~~ <sup>or the identities of confidential foreign sources,</sup> required by Section 3-303 of the Order, the need to protect the information shall be presumed to predominate.

3-404  
(2) Systematic Review. Within one year after the effective date of the Order, heads of affected agencies shall, in accordance with the provisions of Section 3-404 of the Order, develop guidelines for the systematic review of 30-year old foreign government information. These guidelines shall be kept current through review by concerned agency heads at least once every five years unless earlier review for revision is requested by the Archivist of the United States. A copy of these guidelines and any revisions thereto shall be furnished to the Information Security Oversight Office. If, after applying the guidelines to 30-year old foreign government information, a determination is made by the reviewer that continued classification would be appropriate, a date no more than ten years later shall be set for the next review. That date shall be marked on the document. Subsequent review dates shall be set at no more than ten year intervals.

3-501  
(1) Mandatory Review. Requests for mandatory review for the

declassification of classified documents that contain foreign government information shall be processed and acted upon in accordance with the provisions of Section IV. D. hereof except that foreign government information will be declassified only in accordance with the guidelines developed for the purpose under (2) above. In those cases where these guidelines cannot be applied to the foreign government information requested or, in the absence of such guidelines, consultation with the foreign originator through appropriate channels may be <sup>advisable</sup> necessary prior to final action on the request. However, in those cases where the Agency receiving the request for mandatory review is knowledgeable of the foreign originator's <sup>view</sup> disposition toward declassification or continued classification of the types of information requested based on set precedent, consultation with the foreign originator shall not be necessary.

4-201  
D. Safeguards.

(1) Special Access Programs. Special access programs to protect foreign government information that are set up under a treaty or international agreement do not terminate automatically every five years unless renewed. These special access programs are continued as required by the treaty or agreement and will be reviewed at least once every five years to determine whether the treaty or agreement obligations are being met. An international agreement in this context includes an exchange of letters, a memorandum of understanding and other informal written arrangements between the United States and another government. Such arrangements may be reflected by a writing executed by either government.

... also  
country  
need

~~Appointees. The waiver permitted by Section 4-301 of the Order does~~  
Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
~~not apply to foreign government information.~~

2

1

MONDAY, JULY 3, 1978

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

PART IV



## THE PRESIDENT

### NATIONAL SECURITY INFORMATION

Executive Order 12065  
and Order Designating  
Certain Officials  
Within the Executive  
Office of the President  
To Classify  
Information



# presidential documents

[3195-01]

## Title 3—The President

Executive Order 12065

June 28, 1978

### National Security Information

By the authority vested in me as President by the Constitution and laws of the United States of America, in order to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure, it is hereby ordered as follows:

#### TABLE OF CONTENTS

	[FR page]
<b>SECTION 1. ORIGINAL CLASSIFICATION:</b>	
1-1 Classification Designation .....	[28950]
1-2 Classification Authority .....	[28950]
1-3 Classification Requirements .....	[28951]
1-4 Duration of Classification .....	[28952]
1-5 Identification and Markings .....	[28952]
1-6 Prohibitions .....	[28953]
<b>SECTION 2. DERIVATIVE CLASSIFICATION:</b>	
2-1 Use of Derivative Classification .....	[28953]
2-2 Classification Guides .....	[28953]
2-3 New Material .....	[28954]
<b>SECTION 3. DECLASSIFICATION AND DOWNGRADING:</b>	
3-1 Declassification Authority .....	[28954]
3-2 Transferred Information .....	[28954]
3-3 Declassification Policy .....	[28955]
3-4 Systematic Review for Declassification .....	[28955]
3-5 Mandatory Review for Declassification .....	[28956]
3-6 Downgrading .....	[28957]
<b>SECTION 4. SAFEGUARDING:</b>	
4-1 General Restrictions .....	[28957]
4-2 Special Access Programs .....	[28957]
4-3 Access by Historical Researchers and Former Presidential Appointees .....	[28958]
4-4 Reproduction Controls .....	[28958]
<b>SECTION 5. IMPLEMENTATION AND REVIEW:</b>	
5-1 Oversight .....	[28959]
5-2 Information Security Oversight Office .....	[28959]
5-3 Interagency Information Security Committee .....	[28960]
5-4 General Responsibilities .....	[28960]
5-5 Administrative Sanctions .....	[28961]
<b>SECTION 6. GENERAL PROVISIONS:</b>	
6-1 Definitions .....	[28961]
6-2 General .....	[28961]

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
SECTION 1. ORIGINAL CLASSIFICATION.

1-1. *Classification Designation.*

1-101. Except as provided in the Atomic Energy Act of 1954, as amended, this Order provides the only basis for classifying information. Information may be classified in one of the three designations listed below. If there is reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive designation should be used, or the information should not be classified.

1-102. "Top Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

1-103. "Secret" shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

1-104. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause identifiable damage to the national security.

1-2. *Classification Authority.*

1-201. *Top Secret.* Authority for original classification of information as Top Secret may be exercised only by the President, by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, and by officials to whom such authority is delegated in accordance with Section 1-204:

- The Secretary of State
- The Secretary of the Treasury
- The Secretary of Defense
- The Secretary of the Army
- The Secretary of the Navy
- The Secretary of the Air Force
- The Attorney General
- The Secretary of Energy
- The Chairman, Nuclear Regulatory Commission
- The Director, Arms Control and Disarmament Agency
- The Director of Central Intelligence
- The Administrator, National Aeronautics and Space Administration
- The Administrator of General Services (delegable only to the Director, Federal Preparedness Agency and to the Director, Information Security Oversight Office)

1-202. *Secret.* Authority for original classification of information as Secret may be exercised only by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, by officials who have Top Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:

- The Secretary of Commerce
- The Secretary of Transportation
- The Administrator, Agency for International Development
- The Director, International Communication Agency

1-203. *Confidential.* Authority for original classification of information as Confidential may be exercised only by such officials as the President may designate by publication in the FEDERAL REGISTER, by the agency heads listed below, by officials who have Top Secret or Secret classification authority, and by officials to whom such authority is delegated in accordance with Section 1-204:

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
 The President and Chairman, Export-Import Bank of the United States  
 The President and Chief Executive Officer, Overseas Private Investment Corporation

*1-204. Limitations on Delegation of Classification Authority.*

(a) Authority for original classification of information as Top Secret may be delegated only to principal subordinate officials who have a frequent need to exercise such authority as determined by the President or by agency heads listed in Section 1-201.

(b) Authority for original classification of information as Secret may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201 and 1-202, and by officials with Top Secret classification authority.

(c) Authority for original classification of information as Confidential may be delegated only to subordinate officials who have a frequent need to exercise such authority as determined by the President, by agency heads listed in Sections 1-201, 1-202, and 1-203, and by officials with Top Secret classification authority.

(d) Delegated original classification authority may not be redelegated.

(e) Each delegation of original classification authority shall be in writing by name or title of position held.

(f) Delegations of original classification authority shall be held to an absolute minimum. Periodic reviews of such delegations shall be made to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

*1-205. Exceptional Cases.* When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be protected in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority. That agency shall decide within 30 days whether to classify that information. If it is not clear which agency should get the information, it shall be sent to the Director of the Information Security Oversight Office established in Section 5-2 for a determination.

*1-3. Classification Requirements.*

*1-301.* Information may not be considered for classification unless it concerns:

- (a) military plans, weapons, or operations;
- (b) foreign government information;
- (c) intelligence activities, sources or methods;
- (d) foreign relations or foreign activities of the United States;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities; or
- (g) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President, by a person designated by the President pursuant to Section 1-201, or by an agency head.

*1-302.* Even though information is determined to concern one or more of the criteria in Section 1-301, it may not be classified unless an original classification authority also determines that its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security.

THE PRESIDENT

1-303. Unauthorized disclosure of foreign government information or the identity of a confidential foreign source is presumed to cause at least identifiable damage to the national security.

1-304. Each determination under the criterion of Section 1-301(g) shall be reported promptly to the Director of the Information Security Oversight Office.

*1-4. Duration of Classification.*

1-401. Except as permitted in Section 1-402, at the time of the original classification each original classification authority shall set a date or event for automatic declassification no more than six years later.

1-402. Only officials with Top Secret classification authority and agency heads listed in Section 1-2 may classify information for more than six years from the date of the original classification. This authority shall be used sparingly. In such cases, a declassification date or event, or a date for review, shall be set. This date or event shall be as early as national security permits and shall be no more than twenty years after original classification, except that for foreign government information the date or event may be up to thirty years after original classification.

*1-5. Identification and Markings.*

1-501. At the time of original classification, the following shall be shown on the face of paper copies of all classified documents:

- (a) the identity of the original classification authority;
- (b) the office of origin;
- (c) the date or event for declassification or review; and
- (d) one of the three classification designations defined in Section 1-1.

1-502. Documents classified for more than six years shall also be marked with the identity of the official who authorized the prolonged classification. Such documents shall be annotated with the reason the classification is expected to remain necessary, under the requirements of Section 1-3, despite the passage of time. The reason for the prolonged classification may be stated by reference to criteria set forth in agency implementing regulations. These criteria shall explain in narrative form the reason the information needs to be protected beyond six years. If the individual who signs or otherwise authenticates a document also is authorized to classify it, no further annotation of identity is required.

1-503. Only the designations prescribed by this Order may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" may not be used for that purpose. Terms such as "Conference" or "Agency" may not be used in conjunction with the classification designations prescribed by this Order; e.g., "Agency Confidential" or "Conference Confidential."

1-504. In order to facilitate excerpting and other uses, each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified. The Director of the Information Security Oversight Office may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information.

1-505. Foreign government information shall either retain its original classification designation or be assigned a United States classification designation that shall ensure a degree of protection equivalent to that required by the entity that furnished the information.

1-506. Classified documents that contain or reveal information that is subject to special dissemination and reproduction limitations authorized by

this Order shall be marked clearly so as to place the user on notice of the restrictions.

**1-6. Prohibitions.**

1-601. Classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

1-602. Basic scientific research information not clearly related to the national security may not be classified.

1-603. A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Order until and unless the government acquires a proprietary interest in the product. This Order does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181-188).

1-604. References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.

1-605. Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Order or to prevent or delay the public release of such information.

1-606. No document originated on or after the effective date of this Order may be classified after an agency has received a request for the document under the Freedom of Information Act or the Mandatory Review provisions of this Order (Section 3-5), unless such classification is consistent with this Order and is authorized by the agency head or deputy agency head. Documents originated before the effective date of this Order and subject to such a request may not be classified unless such classification is consistent with this Order and is authorized by the senior official designated to oversee the agency information security program or by an official with Top Secret classification authority. Classification authority under this provision shall be exercised personally, on a document-by-document basis.

1-607. Classification may not be restored to documents already declassified and released to the public under this Order or prior Orders.

**SECTION 2. DERIVATIVE CLASSIFICATION.**

**2-1. Use of Derivative Classification.**

2-101. Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide.

2-102. Persons who apply such derivative classification markings shall:

- (a) respect original classification decisions;
- (b) verify the information's current level of classification so far as practicable before applying the markings; and
- (c) carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings, in accordance with Sections 2-2 and 2-301 below. A single marking may be used for documents based on multiple sources.

**2-2. Classification Guides.**

2-201. Classification guides used to direct derivative classification shall specifically identify the information to be classified. Each classification guide shall specifically indicate how the designations, time limits, markings, and other requirements of this Order are to be applied to the information.

2-202. Each such guide shall be approved personally and in writing by an agency head listed in Section 1-2 or by an official with Top Secret classification authority. Such approval constitutes an original classification decision.

2-3. *New Material.*

2-301. New material that derives its classification from information classified on or after the effective date of this Order shall be marked with the declassification date or event, or the date for review, assigned to the source information.

2-302. New material that derives its classification from information classified under prior Orders shall be treated as follows:

(a) If the source material bears a declassification date or event twenty years or less from the date of origin, that date or event shall be carried forward on the new material.

(b) If the source material bears no declassification date or event or is marked for declassification beyond twenty years, the new material shall be marked with a date for review for declassification at twenty years from the date of original classification of the source material.

(c) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond thirty years, the new material shall be marked for review for declassification at thirty years from the date of original classification of the source material.

SECTION 3. DECLASSIFICATION AND DOWNGRADING.

3-1. *Declassification Authority.*

3-101. The authority to declassify or downgrade information classified under this or prior Orders shall be exercised only as specified in Section 3-1.

3-102. Classified information may be declassified or downgraded by the official who authorized the original classification if that official is still serving in the same position, by a successor, or by a supervisory official of either.

3-103. Agency heads named in Section 1-2 shall designate additional officials at the lowest practicable echelons to exercise declassification and downgrading authority.

3-104. If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.

3-105. The provisions of this Order relating to declassification shall also apply to agencies which, under the terms of this Order, do not have original classification authority but which had such authority under prior Orders.

3-2. *Transferred Information.*

3-201. For classified information transferred in conjunction with a transfer of functions—not merely for storage purposes—the receiving agency shall be deemed to be the originating agency for all purposes under this Order.

3-202. For classified information not transferred in accordance with Section 3-201, but originated in an agency which has ceased to exist, each agency in possession shall be deemed to be the originating agency for all purposes under this Order. Such information may be declassified or downgraded by the agency in possession after consulting with any other agency having an interest in the subject matter.

3-203. Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be declassi-

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

THE PRESIDENT  
fied or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and the agency guidelines.

3-204. After the termination of a Presidential administration, the Archivist of the United States shall review and declassify or downgrade all information classified by the President, the White House Staff, committees or commissions appointed by the President, or others acting on the President's behalf. Such declassification shall only be undertaken in accordance with the provisions of Section 3-504.

### 3-3. *Declassification Policy.*

3-301. Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to this and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event.

3-302. When information is reviewed for declassification pursuant to this Order or the Freedom of Information Act, it shall be declassified unless the declassification authority established pursuant to Section 3-1 determines that the information continues to meet the classification requirements prescribed in Section 1-3 despite the passage of time.

3-303. It is presumed that information which continues to meet the classification requirements in Section 1-3 requires continued protection. In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head, a senior agency official with responsibility for processing Freedom of Information Act requests or Mandatory Review requests under this Order, an official with Top Secret classification authority, or the Archivist of the United States in the case of material covered in Section 3-503. That official will determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

### 3-4. *Systematic Review for Declassification.*

3-401. Classified information constituting permanently valuable records of the Government, as defined by 44 U.S.C. 2103, and information in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be reviewed for declassification as it becomes twenty years old. Agency heads listed in Section 1-2 and officials designated by the President pursuant to Section 1-201 of this Order may extend classification beyond twenty years, but only in accordance with Sections 3-3 and 3-402. This authority may not be delegated. When classification is extended beyond twenty years, a date no more than ten years later shall be set for declassification or for the next review. That date shall be marked on the document. Subsequent reviews for declassification shall be set at no more than ten year intervals. The Director of the Information Security Oversight Office may extend the period between subsequent reviews for specific categories of documents or information.

3-402. Within 180 days after the effective date of this Order, the agency heads listed in Section 1-2 and the heads of agencies which had original classification authority under prior orders shall, after consultation with the Archivist of the United States and review by the Information Security Oversight Office, issue and maintain guidelines for systematic review covering twenty-year old classified information under their jurisdiction. These guide-

## THE PRESIDENT

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

information, with the exception of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond twenty years is needed. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information. All information not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of twenty years from the date of original classification.

3-403. Notwithstanding Sections 3-401 and 3-402, the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review and declassification of classified information concerning the identities of clandestine human agents. These procedures shall be consistent, so far as practicable, with the objectives of Sections 3-401 and 3-402. Prior to implementation, they shall be reviewed and approved by the Director of the Information Security Oversight Office and, with respect to matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Disapproval of procedures by the Director of the Information Security Oversight Office may be appealed to the National Security Council. In such cases, the procedures shall not be implemented until the appeal is decided.

3-404. Foreign government information shall be exempt from automatic declassification and twenty year systematic review. Unless declassified earlier, such information shall be reviewed for declassification thirty years from its date of origin. Such review shall be in accordance with the provisions of Section 3-3 and with guidelines developed by agency heads in consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned. These guidelines shall be authorized for use by the Archivist of the United States and may, upon approval of the issuing authority, be used by any agency having custody of the information.

3-405. Transition to systematic review at twenty years shall be implemented as rapidly as practicable and shall be completed no more than ten years from the effective date of this Order.

### 3-5. *Mandatory Review for Declassification.*

3-501. Agencies shall establish a mandatory review procedure to handle requests by a member of the public, by a government employee, or by an agency, to declassify and release information. This procedure shall apply to information classified under this Order or prior Orders. Except as provided in Section 3-503, upon such a request the information shall be reviewed for possible declassification, provided the request reasonably describes the information. Requests for declassification under this provision shall be acted upon within 60 days. After review, the information or any reasonably segregable portion thereof that no longer requires protection under this Order shall be declassified and released unless withholding is otherwise warranted under applicable law.

3-502. Requests for declassification which are submitted under the provisions of the Freedom of Information Act shall be processed in accordance with the provisions of that Act.

3-503. Information less than ten years old which was originated by the President, by the White House Staff, or by committees or commissions appointed by the President, or by others acting on behalf of the President, including such information in the possession and control of the Administrator



Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
of General Services pursuant to 44 U.S.C. 2107 or 2107 note, shall be excluded from the provisions of Section 3-501. Such information over ten years old shall be subject to mandatory review for declassification. Requests for mandatory review shall be processed in accordance with procedures developed by the Archivist of the United States. These procedures shall provide for consultation with agencies having primary subject matter interest. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council through the process set forth in Section 3-104.

3-504. Requests for declassification of classified documents originated by an agency but in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be referred by the Archivist to the agency of origin for processing in accordance with Section 3-501 and for direct response to the requestor. The Archivist shall inform requestors of such referrals.

3-505. No agency in possession of a classified document may, in response to a request for the document made under the Freedom of Information Act or this Order's Mandatory Review provision, refuse to confirm the existence or non-existence of the document, unless the fact of its existence or non-existence would itself be classifiable under this Order.

#### 3-6. Downgrading.

3-601. Classified information that is marked for automatic downgrading is downgraded accordingly without notification to holders.

3-602. Classified information that is not marked for automatic downgrading may be assigned a lower classification designation by the originator or by other authorized officials when such downgrading is appropriate. Notice of downgrading shall be provided to holders of the information to the extent practicable.

### SECTION 4. SAFEGUARDING.

#### 4-1. General Restrictions on Access.

4-101. No person may be given access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties.

4-102. All classified information shall be marked conspicuously to put users on notice of its current classification status and, if appropriate, to show any special distribution or reproduction restrictions authorized by this Order.

4-103. Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, and transmitted only under conditions that will provide adequate protection and prevent access by unauthorized persons.

4-104. Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of Chapters 21 and 33 of Title 44 of the United States Code, which governs disposition of Federal records.

4-105. Classified information disseminated outside the Executive branch shall be given protection equivalent to that afforded within the Executive branch.

#### 4-2. Special Access Programs.

4-201. Agency heads listed in Section 1-201 may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or prior Orders. Such pro-

## THE PRESIDENT

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

grams may be created or continued only by written direction and only by those agency heads and, for matters pertaining to intelligence sources and methods, by the Director of Central Intelligence. Classified information in such programs shall be declassified according to the provisions of Section 3.

4-202. Special access programs may be created or continued only on a specific showing that:

(a) normal management and safeguarding procedures are not sufficient to limit need-to-know or access;

(b) the number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information involved; and

(c) the special access controls balance the need to protect the information against the full spectrum of needs to use the information.

4-203. All special access programs shall be reviewed regularly and, except those required by treaty or international agreement, shall terminate automatically every five years unless renewed in accordance with the procedures in Section 4-2.

4-204. Within 180 days after the effective date of this Order, agency heads shall review all existing special access programs under their jurisdiction and continue them only in accordance with the procedures in Section 4-2. Each of those agency heads shall also establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office shall have non-delegable access to all such accountings.

4-3. *Access by Historical Researchers and Former Presidential Appointees.*

4-301. The requirement in Section 4-101 that access to classified information may be granted only as is necessary for the performance of official duties may be waived as provided in Section 4-302 for persons who:

(a) are engaged in historical research projects, or

(b) previously have occupied policy-making positions to which they were appointed by the President.

4-302. Waivers under Section 4-301 may be granted only if the agency with jurisdiction over the information:

(a) makes a written determination that access is consistent with the interests of national security;

(b) takes appropriate steps to ensure that access is limited to specific categories of information over which that agency has classification jurisdiction;

(c) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed or received while serving as a Presidential appointee.

4-4. *Reproduction Controls.*

4-401. Top Secret documents may not be reproduced without the consent of the originating agency unless otherwise marked by the originating office.

4-402. Reproduction of Secret and Confidential documents may be restricted by the originating agency.

4-403. Reproduced copies of classified documents are subject to the same accountability and controls as the original documents.

4-404. Records shall be maintained by all agencies that reproduce paper copies of classified documents to show the number and distribution of reproduced copies of all Top Secret documents, of all documents covered by special access programs distributed outside the originating agency, and of all Secret and all Confidential documents which are marked with special dissemination and reproduction limitations in accordance with Section 1-506.

4-405. Sections 4-401 and 4-402 shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However,

such reproduced documents that remain classified after review must be destroyed after they are used.

**SECTION 5. IMPLEMENTATION AND REVIEW.**

**5-1. Oversight.**

5-101. The National Security Council may review all matters with respect to the implementation of this Order and shall provide overall policy direction for the information security program.

5-102. The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. This responsibility shall be delegated to an Information Security Oversight Office.

**5-2. Information Security Oversight Office.**

5-201. The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Administrator also shall have authority to appoint a staff for the Office.

**5-202. The Director shall:**

(a) oversee agency actions to ensure compliance with this Order and implementing directives;

(b) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program, including appeals from decisions on declassification requests pursuant to Section 3-503;

(c) exercise the authority to declassify information provided by Sections 3-104 and 3-503;

(d) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order which shall be binding on the agencies;

(e) report annually to the President through the Administrator of General Services and the National Security Council on the implementation of this Order;

(f) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect until the appeal is decided or until one year from the date of the Director's decision, whichever occurs first.

(g) exercise case-by-case classification authority in accordance with Section 1-205 and review requests for original classification authority from agencies or officials not granted original classification authority under Section 1-2 of this Order; and

(h) have the authority to conduct on-site reviews of the information security program of each agency that handles classified information and to require of each agency such reports, information, and other cooperation as necessary to fulfill his responsibilities. If such reports, inspection, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect until the appeal is decided or until one year from the date of the denial, whichever occurs first.

## THE PRESIDENT

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
 5-3. *Interagency Information Security Committee.*

5-301. There is established an Interagency Information Security Committee which shall be chaired by the Director and shall be comprised of representatives of the Secretaries of State, Defense, Treasury, and Energy, the Attorney General, the Director of Central Intelligence, the National Security Council, the Domestic Policy Staff, and the Archivist of the United States.

5-302. Representatives of other agencies may be invited to meet with the Committee on matters of particular interest to those agencies.

5-303. The Committee shall meet at the call of the Chairman or at the request of a member agency and shall advise the Chairman on implementation of this order.

5-4. *General Responsibilities.*

5-401. A copy of any information security regulation and a copy of any guideline for systematic declassification review which has been adopted pursuant to this Order or implementing directives, shall be submitted to the Information Security Oversight Office. To the extent practicable, such regulations and guidelines should be unclassified.

5-402. Unclassified regulations that establish agency information security policy and unclassified guidelines for systematic declassification review shall be published in the FEDERAL REGISTER.

5-403. Agencies with original classification authority shall promulgate guides for security classification that will facilitate the identification and uniform classification of information requiring protection under the provisions of this Order.

5-404. Agencies which originate or handle classified information shall:

(a) designate a senior agency official to conduct an active oversight program to ensure effective implementation of this Order;

(b) designate a senior agency official to chair an agency committee with authority to act on all suggestions and complaints with respect to the agency's administration of the information security program;

(c) establish a process to decide appeals from denials of declassification requests submitted pursuant to Section 3-5;

(d) establish a program to familiarize agency and other personnel who have access to classified information with the provisions of this Order and implementing directives. This program shall impress upon agency personnel their responsibility to exercise vigilance in complying with this Order. The program shall encourage agency personnel to challenge, through Mandatory Review and other appropriate procedures, those classification decisions they believe to be improper;

(e) promulgate guidelines for systematic review in accordance with Section 3-402;

(f) establish procedures to prevent unnecessary access to classified information, including procedures which require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and which ensures that the number of people granted access to classified information is reduced to and maintained at the minimum number that is consistent with operational requirements and needs; and

(g) ensure that practices for safeguarding information are systematically reviewed and that those which are duplicative or unnecessary are eliminated.

5-405. Agencies shall submit to the Information Security Oversight Office such information or reports as the Director of the Office may find necessary to carry out the Office's responsibilities.

5-5. *Administrative Sanctions.*

5-501. If the Information Security Oversight Office finds that a violation of this Order or any implementing directives may have occurred, it shall make a report to the head of the agency concerned so that corrective steps may be taken.

5-502. Officers and employees of the United States Government shall be subject to appropriate administrative sanctions if they:

- (a) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directives; or
- (b) knowingly, willfully and without authorization disclose information properly classified under this Order or prior Orders or compromise properly classified information through negligence; or
- (c) knowingly and willfully violate any other provision of this Order or implementing directive.

5-503. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations.

5-504. Agency heads shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5-502 occurs. The Director of the Information Security Oversight Office shall be informed when such violations occur.

5-505. Agency heads shall report to the Attorney General evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.

SECTION 6. GENERAL PROVISIONS.

6-1. *Definitions.*

6-101. "Agency" has the meaning defined in 5 U.S.C. 552(e).

6-102. "Classified information" means information or material, herein collectively termed information, that is owned by, produced for or by, or under the control of, the United States Government, and that has been determined pursuant to this Order or prior Orders to require protection against unauthorized disclosure, and that is so designated.

6-103. "Foreign government information" means information that has been provided to the United States in confidence by, or produced by the United States pursuant to a written joint arrangement requiring confidentiality with, a foreign government or international organization of governments.

6-104. "National security" means the national defense and foreign relations of the United States.

6-105. "Declassification event" means an event which would eliminate the need for continued classification.

6-2. *General.*

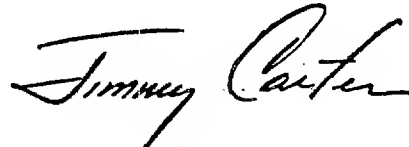
6-201. Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and information designated as "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued pursuant thereto.

6-202. The Attorney General, upon request by the head of an agency, his duly designated representative, or the Director of the Information Security Oversight Office, shall personally or through authorized representatives of the Department of Justice render an interpretation of this Order with respect to any question arising in the course of its administration.

## THE PRESIDENT

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5  
6-203. Executive Order No. 11652 of March 8, 1972, as amended by Executive Order No. 11714 of April 24, 1973, and as further amended by Executive Order No. 11862 of June 11, 1975, and the National Security Council Directive of May 17, 1972 (3 CFR 1085 (1971-75 Comp.)) are revoked.

6-204. This Order shall become effective on December 1, 1978, except that the functions of the Information Security Oversight Office specified in Sections 5-202(d) and 5-202(f) shall be effective immediately and shall be performed in the interim by the Interagency Classification Review Committee established pursuant to Executive Order No. 11652.



THE WHITE HOUSE,  
*June 28, 1978.*

[FR Doc. 78-18505 Filed 6-29-78; 4:18 pm]

EDITORIAL NOTE: The President's statement of June 29, 1978, on issuing Executive Order 12065, is printed in the Weekly Compilation of Presidential Documents (vol. 14, No. 26).

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

[3195-01]

Order of June 28, 1978

Designation of Certain Officials Within the Executive Office of the President To Classify  
National Security Information

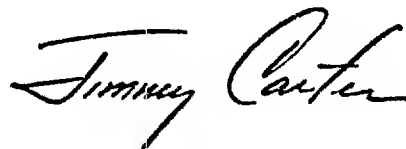
Pursuant to the provisions of Section 1-201 of Executive Order 12065 of June 28, 1978, entitled "National Security Information", I hereby designate the following officials within the Executive Office of the President to originally classify information as "Top Secret"

- The Vice President
- The Assistant to the President for National Security Affairs
- The Director, Office of Management and Budget
- The Director, Office of Science and Technology Policy
- The Special Representative for Trade Negotiations
- The Chairman, Intelligence Oversight Board

Pursuant to the provisions of Section 1-202 of said Order, I designate the Chairman of the Council of Economic Advisers and the President's Personal Representative for Micronesian Status Negotiations to originally classify information as "Secret".

Any delegation of this authority shall be in accordance with Section 1-204 of the Order.

This Order shall be published in the FEDERAL REGISTER.



THE WHITE HOUSE,  
June 28, 1978.

[FR Doc. 78-18508 Filed 6-29-78; 4:19 pm]

Approved For Release 2001/08/09 : CIA-RDP94B01041R000300010001-5

SECTION I. ORIGINAL CLASSIFICATION

F. (1) Date of Classification and Office of Origin and

F. (2) Identity of Classifier.

We recognize that this is a document to be coordinated with NSC. We assume that the language in Section I. F. (1) takes precedence over the language in Section I F. (2) so that the Agency can continue to use employee numbers to identify its classifiers when necessary for cover purposes, instead of using names as required in Section I F. (2).



SECTION II. DERIVATIVE APPLICATIONS OF CLASSIFICATION MARKINGS

B. Responsibility.

The last sentence here states, "Where checks with originators or other appropriate inquiries show that no classification or a lower classification than originally assigned is appropriate, the information shall be marked accordingly." What the other "appropriate inquiries" would be is not made clear. It seems to us that this could lead to improper downgrading of properly classified material by non-technical personnel who simply might not be aware of a need for continued classification of certain items. We believe the downgrading authority should remain with the originating office, and that this should be clearly stated here. We recommend that the phrase "or other appropriate inquiries" be struck from Section II. B.

SECTION IV. OTHER CLASSIFICATION ACTIONS AND NOTICES

D. Extension of Duration of Classification (DOD additional recommendations 1 - 401)

This paragraph states, "The duration of classification specified at the time of original classification may be extended by officials with requisite authority but only if notification of such action can be received by all known holders of the information prior to the date or event previously set for automatic declassification." We believe we understand the intent here, but the language leaves no room for any last minute judgment. We see the possibility that information which truly should remain classified will be downgraded or declassified simply because it has been sent to such a large audience that they cannot all be notified in time. We recommend instead, the following wording: "The duration of classification specified at the time of original classification may be extended by officials with requisite authority, but at the same time they must make every reasonable effort to notify all known holders of the information prior to the date or the event previously set for automatic downgrading or declassification." This approach seems to us to be more consistent with Section IV.C. (1-606) of the DOD additional recommendations, which would permit classification of previously unclassified material if control of the information has not yet been lost.

**SENDER WILL CHECK CLASSIFICATION TOP AND BOTTOM**

~~Approved For Release~~  
**UNCLASSIFIED**

~~CONFIDENTIAL~~

**SECRET**

## OFFICIAL ROUTING SLIP

TO	NAME AND ADDRESS		DATE	INITIALS
1	Executive Order 12065 File			
2				
3				
4				
5				
6				
	ACTION	DIRECT REPLY	PREPARE REPLY	
	APPROVAL	DISPATCH	RECOMMENDATION	
	COMMENT	FILE	RETURN	
	CONCURRENCE	INFORMATION	SIGNATURE	

Remarks:

These are the combined comments of DSB  
[redacted] and ISB ([redacted]) forwarded on  
24 July 78 to PPG/OS, concerning the E.O. 12065  
Implementing Instructions (Draft.) (12 Jul 78)

**TO RETURN TO SENDER**

ESS AND PHONE NO.

DATE \_\_\_\_\_

24 Jul 78

**UNCLASSIFIED**

**CONFIDENTIAL**

**SECRET**